



FortiAuthenticator - Release Notes

VERSION 5.2.0

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FORTINET PRIVACY POLICY

<https://www.fortinet.com/corporate/about-us/privacy.html>

FEEDBACK

Email: techdocs@fortinet.com



01/15/2018

FortiAuthenticator 5.2.0 - Release Notes

Revision 3

TABLE OF CONTENTS

Introduction	4
Special Notices	5
TFTP boot process	5
Monitor settings for web-based manager access	5
Before any upgrade	5
After any upgrade	5
What's New	6
Upgrade Instructions	9
Hardware & VM support	9
Image checksums	9
Upgrading from FortiAuthenticator 4.x/5.0/5.1	10
Product Integration and Support	12
Web browser support	12
FortiOS support	12
Fortinet agent support	12
Virtualization software support	13
Third party RADIUS authentication	13
Resolved Issues	14
Known Issues	16
Appendix A: FortiAuthenticator VM	18
FortiAuthenticator VM system requirements	18
FortiAuthenticator VM firmware	18
Appendix B: Maximum values	19
Hardware appliances	19
VM appliances	21

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator™ 5.2.0, build 0155.

FortiAuthenticator is a User and Identity Management solution that provides Strong Authentication, Wireless 802.1X Authentication, Certificate Management, and Fortinet Single Sign-On.

For additional documentation, please visit:

<http://docs.fortinet.com/fortiauthenticator/>

Special Notices

TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the Web-based Manager to be viewed properly without need for scrolling.

Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. Go to *System > Dashboard > Status* and select *Backup/Restore > Download backup file* to backup the configuration.

After any upgrade

If you are using the Web-based Manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the Web-based Manager screens are displayed properly.

What's New

Before upgrading, review the following changes for impact to your unique deployment. This list highlights the major feature enhancements in this release.

Guest Portals

The following new features are introduced for Guest Portals in this release:

Disclaimer update

In order to increase parity with captive portal offerings, the guest portal now offers the option to present a disclaimer to the end-user that must be accepted before proceeding to the login page.

The disclaimer is enabled in the *Pre-login Services* section of the portal configuration under *Authentication > Guest Portals > Portals*.

The disclaimer page is a new guest portal replacement message configurable under the "Authentication" section named "Login Disclaimer Page". This new replacement has the same description and HTML code as the one for the legacy captive portal (*Authentication > Guest Portals > Replacement Messages*).

Exceeded usage handling (446146)

Previously, when a user exceeded their utilisation profile, a disconnect message was sent from the FAC to the FGT. The user was then disabled on the FAC and could not log back in.

This feature allows the administrator to configure a notification to inform the user as to why they've been disconnected (because their usage profile has been exceeded) and to provide a mechanism where the user can *Request Usage Extension*. The *Request Usage Extension* button will email a notification to a pre-configured email address under *Authentication > Guest Portals > Portals*.

The GUI checks the lockout reason to determine whether to display an alternate message to the user. As part of remediation, the administrator now also has the option to clear usage data associated with a user.

Smart Connect Profiles

This feature provides the ability to set up network settings (such as WiFi configuration) on an endpoint by downloading a script or an executable, depending on the endpoint's OS, via the FAC's guest portal.

The Smart Connect feature will show up as a new button on the guest portal's post-login main page:



When clicking on the Smart Connect button, the user is given the option to download a self-install file for the OS of their choice.

In this initial release, iOS and MacOS are supported.

Social login

To further increase parity with legacy captive portals, social login is added to the guest portal feature under *Authentication > Guest Portals > Portals*.

In order to give the option to return specific RADIUS attributes for successful social login authentications, the *Profile Configuration* table now offers the ability to specify the user group to use for social (and device-only) logins for each RADIUS client. This user group field is optional, even when social or device-only login is enabled.

A few relevant Replacement Messages have been added:

- **Social Login Page:**
HTML for login page when social login is enabled.
- **Social Mobile/Email Verification Page:**
HTML for guest to input mobile number or email address for login using mobile or email verification.
- **Social Mobile/Email Verification Message:**
Message sent to user for mobile or email verification.
- **Social Email Verification Page:**
HTML for email verification page.
- **Social Mobile Verification Page:**
HTML for mobile number verification page.
- **Social Network Plus FAC Accounts:**
HTML for guest portal social authentication login page which also includes simple login page.

When only *Account Login* is enabled, the guest portal presents the existing "Login Page" replacement message. When *Social Login* is enabled, the guest portal presents the new "Social Login Page" replacement message. When both *Account Login* and *Social Login* are enabled, the guest portal presents the new "Social Network Plus FAC Accounts" replacement message.

MAC-only authentication

The option has been added to perform device-only authentication on the guest portals under *Authentication > Guest Portals > Portals*.

By default, *User credentials* is selected. When the *Device only (MAC address)* option is selected, the "MAC device HTTP parameter" option must also be configured.

When the *Device only (MAC address)* option is enabled, the endpoint will not be presented with the login page. Instead, the FAC will only use the endpoint device's MAC address for authentication purposes. If the RADIUS client profile associated has *MAC device filtering* enabled, the MAC address is authenticated according to those settings. If *MAC device filtering* is disabled, any MAC address is accepted.

A new guest portal Replacement Message is introduced accordingly:

- **Unauthorized Device Page:**
HTML page presented on a failed device-only authentication attempt.

REST API enhancements

In preparation for an upcoming AaaS feature called FortiAuthentication Service (FAS), the REST API is enhanced to handle pushauth requests originating from FAS clients.

Configurable password renewal notification (376122)

Password renewal notification timing is now configurable. Password renewal notifications were previously hard-coded to be sent 14 days, 7 days, 3 days, and 1 day before password expiry.

The new option to configure password renewal notifications to any other combination (other than the defaults of 14, 7, 3, and 1) can be found under *Authentication > User Account Policies > Passwords > User Password Renewal Policy*.

Remote logging using IPv6 (424243)

Added support for IPv6 remote logging through FortiAnalyzer and Syslog.

FSSO: IPv6 support (367159)

Added support for injection of IPv6 addresses using Syslog-to-FSSO and API-to-FSSO (the IPv6 addresses will no longer be rejected by the backend parsing engine).

In addition to Syslog and API, we also implemented RADIUS accounting, SSO login portal, Kerberos, FortiClient Mobility Agent and Windows AD Event Polling. Support for DC/TS agent is ready, but agents were still being developed at the time of release.

FTM: New PIN policy option

Two new options for PIN policy are now offered (in addition to the "Not required" option) under *System > Administration > FortiGuard > FortiToken Mobile Provisioning*:

- **Required:**
User has the option to set App PIN and delete App PIN. If user does not set App PIN or delete App PIN, FTM opens without any protection because it does not have any App protection.
- **Enforced:**
User must set App PIN and cannot delete App PIN. User will always be asked to enter App PIN or TouchID based on settings in the App.

Upgrade Instructions



Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator™ configuration, see the [FortiAuthenticator Administration Guide](#).

Hardware & VM support

FortiAuthenticator™ 5.2.0 supports:

- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000C
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000B
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, and Xen)

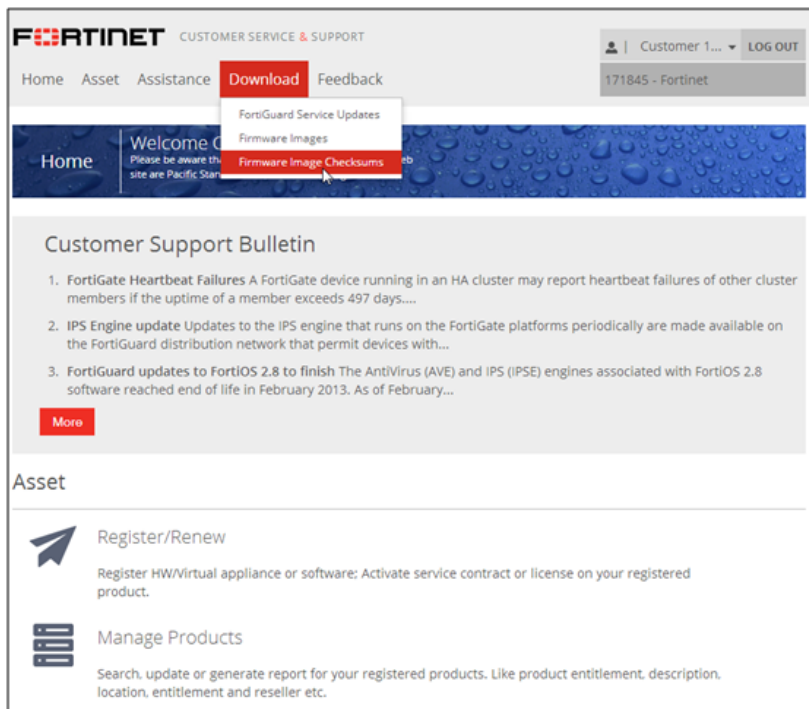
Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

<https://support.fortinet.com>

Customer Service & Support image checksum tool



After logging in to the web site, in the menus at the top of the page, click *Download*, then click *Firmware Image Checksums*.

Alternatively, near the bottom of the page, click the *Firmware Image Checksums* button. (The button appears only if one or more of your devices has a current support contract.) In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.

Upgrading from FortiAuthenticator 4.x/5.0/5.1

FortiAuthenticator™ 5.2.0 build 0155 officially supports upgrade from all versions of FortiAuthenticator™ 4.x.x., 5.0.x, and 5.1.x.



Upgrading the FortiAuthenticator 3000D from 4.0.x to 4.1.x is not supported. The workaround for this model is to upgrade from any 4.0.x version directly to 4.2.0 or higher (skipping all 4.1.x versions).

If you install 4.1.x firmware on a FortiAuthenticator 3000D it stops responding. You can get the system running again by restoring valid firmware using the TFTP boot process.

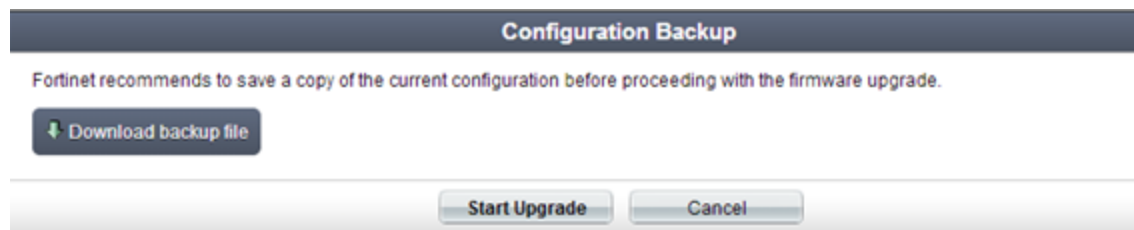
Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator™ firmware, you must download the firmware package from the Customer Service & Support web site, then upload it from your computer to the FortiAuthenticator™ unit.

1. Log in to the Customer Service & Support web site at <https://support.fortinet.com>. In the Download section of the page, select the Firmware Images link to download the firmware.
2. To verify the integrity of the download, go back to the Download section of the login page, then click the *Firmware Image Checksums* link.
3. Log in to the FortiAuthenticator unit's Web-based Manager using the *admin* administrator account.
4. Go to *System > Dashboard > Status*.
5. In the *System Information* widget, in the *Firmware Version* row, select *Upgrade*. The *Firmware Upgrade or Downgrade* dialog box opens.
6. In the *Firmware* section, select *Choose File*, and locate the upgrade package that you downloaded.
7. Select *OK* to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



It is recommended that a system backup is taken at this point. Once complete, click *Start Upgrade*.

Wait until the unpacking, upgrade and reboot process completes (usually 3-5 minutes), then refresh the page.

Product Integration and Support

Web browser support

The following web browsers are supported by FortiAuthenticator™ 5.2.0:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 38
- Mozilla Firefox versions 18 to 54
- Google Chrome versions 28 to 59 (see note below)

Special Note for Google Chrome users



There is a known bug which exists in Google Chrome versions 44 and 45 where initially the GUI loads correctly, however after some time, pages will stop loading with the error on the chrome debug console *"Failed to load resource: net::ERR_INSECURE_RESPONSE"*.

This is a known issue and affects all sites using self-signed certificates and is fixed in Google Chrome version 46. Chrome bug reference:

<https://code.google.com/p/chromium/issues/detail?id=516808>

To work around this issue in the meantime, use a different browser or Upgrade to the Chrome Beta Channel.

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator™ 5.2.0 supports the following FortiOS versions:

- FortiOS v5.2.11
- FortiOS v5.4.5
- FortiOS v5.6.0

Other FortiOS versions may function correctly, but may not be supported by Fortinet.

Fortinet agent support

FortiAuthenticator™ 5.2.0 supports the following Fortinet Agents:

- FortiClient v.5.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.0.2

- FortiAuthenticator Agent for Outlook Web Access 1.4.0
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but may not be supported by Fortinet.

For details of which Operating Systems are supported by each Agent, please see the Install Guides provided with the software.

Virtualization software support

FortiAuthenticator™ 5.2.0 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0
- Microsoft Hyper-V 2010 and Microsoft Hyper-V 2012 R2
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM and AWS)



Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See [Appendix A: FortiAuthenticator VM](#) for more information.

Third party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS). For more information, see the [FortiAuthenticator Two-Factor Authentication Interoperability Guide](#).

Resolved Issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please Fortinet Customer Service & Support:

<https://support.fortinet.com>.

This patch release fixes the following issues found in the release of 5.1.2.

Bug ID	Category	Description
466311	RADIUS auth	Enable Window AD authentication not working as expected
462369	RADIUS auth	802.1x Auth failing on Windows 10 when logging in as remote users using Windows AD domain authentication
466176	FSSO	RADIUS accounting daemon can crash for short-lived sessions when user is disabled
450139	FSSO	FAC RSSO to SSO processing issues and signal 11 crashes of FSSO
451789	FSSO	RSSO not working with sub-domain user via Global Catalog
450441	FSSO	Secondary LDAP server is not used for RSSO group resolution
458772	FSSO	FAC removes a logged in user if it detects more than one IP address assigned to the same user
462849	FSSO	EventID 4624 Network logon (type 3) are caught by FSSO and cause user logouts /flapping on workstation
464454	FSSO	FortiGate SSO monitoring fails when strong crypto is enabled
463168	FAC Agent – Windows	B0012: FAC Agent 2.0.2 for Windows receiving 400 Bad Request when attempting GetOfflineTokens
463550	FAC Agent – Windows	Offline token REST API doesn't support identical usernames across realms (same-kind)
464584	FAC Agent – Outlook	OWA Agent setting allowing users without assigned tokens to authenticate is broken for blank token
433858	FAC-VM	VMware ESXi: virtual serial port does not work
462131	LDAP	Strong Crypto for 389 & 636 (LDAP & LDAPS)
456167	Guest Portal	Support guest portal token bypass when RADIUS client set to use CHAP/MSCHAP/MSCHAPv2

Bug ID	Category	Description
455699	Guest Portal	Guest portal login fails when using FortiCloud with push-notifications
458132	GUI	FAC does not accept email address with TLD longer than 6 characters
463586	GUI	Loading RADIUS Sessions page (under Monitor section) gives a system error
457316	GUI	FortiAuthenticator - CVE-2016-2183 SSL/HTTP and SSL/FSAE are vulnerable against Sweet32
461579	GUI	Firmware version - patch not updated in 5.1.1 and 5.1.2
463650	GUI	Keytab cannot be imported - Invalid keytab file
409345	GUI	When the "Self-service Portal" is enabled, a user (remote user) with admin access can not log into FAC with 2FA
412675	SSH	OpenSSH 7.6 release

Known Issues

This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

There are no known issues at this time.

Bug ID	Category	Description
452878	Certificates	B0226: incorrect number of revoked certificates in CRLs
464094	CLI	Router entry index increase with every edit
452967	CLI	Error when setting allowed-hosts: bad option in substitution expression
394402	FAC Agent – Outlook	OWA Agent does not work with Exchange 2016
461439	FAC Agent – Outlook	Attempting to access Exchange Admin Center redirects to /OWA instead if 2FA is enabled on Outlook Agent
392565	FAC Agent – Windows	Changing the user's FTK doesn't trigger redownloading of all offline tokens
289457	FAC Agent – Windows	FAC Windows Agent not pre-filling RDP domain in some circumstances
404902	FAC Agent – Windows	B0155: FortiAuthenticator Agent for MSWindows: Domain Name contains hyphen, doesn't work correctly
451841	FAC Agent – Windows	B0012: FAC Agent service fails to start and/or disconnects after windows update
463436	FAC Agent – Windows	FAC Windows & OWA Agents need to use TLS 1.2 to communicate with FAC
449443	FAC Agent – Windows	FortiAuthenticator Agent For Microsoft Windows does not display the user credentials when accessing the server through RDP
463972	FSSO	RADIUS accounting log shows a 'Failed to connect to FSSO server' error every second when no RADIUS accounting source is set up
461156	FSSO	The FCT/SSOMA and DC agent overwrite each other's FSSO IP information
460319	FTM Push	Push notifications aren't being sent out to remote admin users

Bug ID	Category	Description
464657	GUI	User Login Password Reset
456296	GUI	Unable to add another attribute to RADIUS Custom Dictionaries
447286	GUI	Enter Valid IP address error message for secondary LDAP GUI configuration; FQDN cannot be used
449324	GUI	B0226: Cannot delete root CA
461885	GUI	Invalid custom dictionary breaks the FAC
452042	GUI	B0012: Using IE11 to display/export the Guest user info doesn't work properly
451555	GUI	Self-Registration with SMS; if the user does not receive the SMS, they are deactivated
462772	GUI	Demoting a remote admin account who has a FTK assigned to a user account causes system error
444829	GUI	RBA Issue: "Role" Section is visible even though FAC admin has no permission to edit options
452280	GUI	FAC 5.0: Import Remote LDAP Users by Group Members; "More" and "All" buttons not working
463849	RADIUS Auth	B0091: FAC Remote LDAP user authentication via RADIUS fails on invalid token if password change and 2FA are required together
381643	RADIUS Auth	EAP authentication fails for remote RADIUS users within two scenarios
399417	RADIUS Auth	FAC 0019 (v4.0): Failover to secondary LDAP server does not occur immediately, and then is not effective
450478	SAML IdP	SAML IdP login failed for user with long DN
463529	SAML IdP	FAC SAML IdP support for Desktop/Thick O365 clients
462184	SAML IdP	SAML IdP does not support saml2p prefix

Appendix A: FortiAuthenticator VM

FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator VM system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported virtual machine (VM) environment. For details, see the *Install Guide for FortiAuthenticator VM* available at <http://docs.fortinet.com>.

VM Requirements

Virtual Machine	Requirement
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Virtual CPUs Supported (Minimum / Maximum)	1 / 8
Virtual NICs Supported (Minimum / Maximum)	1 / 4
Storage Support (Minimum / Maximum)	60GB / 2TB
Memory Support (Minimum / Maximum)	512 MB / 64GB
High Availability Support	Yes

FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- **.out**
Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip**
Use this image for new VM installations. It contains a deployable Open Virtualization Format (OVF) virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, <http://www.fortinet.com/products/fortiauthenticator/index.html>.

Appendix B: Maximum values

This section lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware and VM configurations.



The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Hardware appliances

The following table describes the maximum values set for the various hardware models.

Feature		FortiAuthenticator Model				
		200E	400E	1000D	2000E	3000E
System						
Network	Static Routes	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20
	SMS Gateways	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20
Administration	SYSLOG Servers	20	20	20	20	20
	User Uploaded Images	30	100	500	1000	2000
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333

Feature		FortiAuthenticator Model				
		200E	400E	1000D	2000E	3000E
	Users (Local + Remote) ¹	500	2000	10000	20000	40000
	User Radius Attributes	1500	6000	30000	60000	120000
	User Groups	50	200	1000	2000	4000
	Group Radius Attributes	150	150	600	6000	120000
	FortiTokens	1000	4000	20000	40000	80000
	FortiToken Mobile Licenses ²	200	200	200	200	200
	LDAP Entries	1000	4000	20000	40000	80000
	Device (MAC-based Auth.)	50	200	1000	2000	4000
	RADIUS Client Profiles	500	2000	10000	20000	40000
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Sync Rule	25	100	500	1000	2000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120000
	FSSO & Dynamic Policies					
FSSO	FSSO Users	500	2000	10000	20000	200000 ³
	FSSO Groups	1000	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	400
	RADIUS Accounting SSO Clients	166	666	3333	6666	13333
	FortiGate Services	50	200	1000	2000	4000
	FortiGate Group Filtering	250	1000	5000	10000	20000
	FSSO Tier Nodes	5	20	100	200	400
	IP Filtering Rules	250	1000	5000	10000	20000

Feature		FortiAuthenticator Model				
		200E	400E	1000D	2000E	3000E
Accounting Proxy	Sources	500	2000	10000	20000	40000
	Destinations	25	100	500	1000	2000
	Rulesets	25	100	500	1000	2000
Certificates						
User Certificates	User Certificates	2500	10000	50000	100000	200000
	Server Certificates	50	200	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50
	Trusted CA Certificates	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	50000	100000	200000

¹ Note that there is one metric used for the number of allowed users which is *Users*. Local Users and Remote Users share the same limit value. This enables Local Users **or** Remote Users to be equal to *Users* or for there to be a mixture of user types, however, the total number of Local and Remote Users cannot exceed the *Users* metric.

² *FortiToken Mobile Licenses* refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

³ For the 3000E, the total number of concurrent SSO Users is set to a higher level to cater for large deployments.

VM appliances

The FortiAuthenticator-VM Appliance is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator VM-Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The Calculating Metric column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of Auth Clients (NAS Devices) that can authenticate to the system is:

$$100 / 10 = 10$$

Where this relative system is not used e.g. for static routes, the *calculating metric* is denoted by a '-'. The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Maximum Values - Virtual Machines

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	SYSLOG Servers	2	20	20	20
	User Uploaded Images	5	Users / 20	5	100
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
User Management	Users (Local + Remote) ¹	5	*****	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	Users x 3	300	15000
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) ²	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	1	Users / 10	10	500

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
	RADIUS Client Profiles	3	Users	100	10000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Sync Rule	1	Users / 20	5	250
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	30	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users / 100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
Accounting Proxy	Sources	3	Users	100	1000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	200	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	2500	10000

¹ Note that there is one metric used for the number of allowed users which is *Users*. Local Users and Remote Users share the same limit value. This enables Local Users **or** Remote Users to be equal to *Users* or for there to be a mixture of user types, however, the total number of Local and Remote Users cannot exceed the *Users* metric.

² *FortiToken Mobile Licenses* refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.



FORTINET®

High Performance Network Security



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.